International Journal of Political Science, Law and International Relations (IJPSLIR)
ISSN(P): 2278-8832; ISSN(E): 2278-8840
Vol. 5, Issue 4, Oct 2015, 15-24

THE DILEMMA IN DEFINING THE MEANING OF "USE" IN PATENT INFRINGEMENT

TIEN-WEI (DANIEL), HWANG

Department of Law, National Chung Hsing University

Zhongzheng Rd., Liujia Dist., Tainan City, Taiwan (R.O.C.)

ABSTRACT

Modern society relies heavily on computer technology. However, we have been casually tossing bits of personal information out into the world for decades, like Frederick S. Lane had said "If everyone throws a single soda can out of the car window, it does not take no long for a highway to look pretty hideous."

Since a computer cannot operate without software, it is no wonder that intellectual property protection of software is crucial not only for the software industry, but for other businesses as well.

In our information age, the protection of data is tremendously important because data is rampantly collected via the internet and evaluated by companies for commercial purposes. Even the world's leading corporations are accused of breaching consumers' data privacy. Thus, should we define the term "use" in privacy same as in patent infringement? In this article, I will introduce some decisions in American and Taiwanese courts about this.

KEYWORD: Use, Patent Infringement, Personal Information Protection Act

If everyone throws a single soda can out of the car window,

it does not take no long for a highway to look pretty hideous.

— Frederick S. Lane—[1]

INTRODUCTION

[1] See Lane, F. S. (2009). *American privacy: The 400-year history of our most contested right*. Boston, Mass: Beacon Press., at 261.

Modern society relies heavily on computer technology. Without software, a computer cannot operate. Software and hardware work in tandem in today's information society. So it is no wonder that intellectual property protection of software is crucial not only for the software industry, but for other businesses as well.

Especially, for the first time since the advent of credit cards, [2] there are new ways to pay that don't involve cash, check or plastic. Most are built on top of the existing payments system, but — courtesy of that hand-held computer in our pockets and purses — offer new vistas for both consumers and tech entrepreneurs. [3]

For consumers, mobile payments mean greater convenience and better security. To our surprise, with the enthusiastic help of consumers themselves, credit card companies and retail business were amassing staggering amounts of personal information.[4] Consequently, patent and privacy protection becomes more important than before.

THE PROBLEM IN SOFTWARE PATENT

Software patents[5] are problematic in three different ways. First, it is controversial whether these patents are useful.[6] For instance, computer programs, whether in source or object code, are protected under copyright in many countries. Copyright protection does not depend on any formalities such as registration or the deposit of copies in the 151 countries party to the Berne Convention for the Protection of Literary and Artistic Works. This means that international copyright protection is automatic - it begins as soon as a work is created.

Second, the bounds of software patentability are unclear.[7] The core part of your software-related innovation may lie in an apparatus, a system, an algorithm, a method, a network, the processing of data or the software itself. This, what

[2] For more information about the invention of cardboard money, please see Lane, F. S., *supra note 1*, at 124.
[3] See Sean Sposito, Goodbye, billfold. Hello, smartphone, available at http://www.ajc.com/news/business/personal-finance/goodbye-billfold-hello-smartphone/nfXNc/(accessed March 2015).
[4] See Lane, F. S. , *supra note 1*, at 149.
[5] Compared to European Union, a computer program as such is abstract and mental in nature and therefore specifically excluded from patentability in Article 52(2)(c) European Patent Convention. If it is run on a computer and produces a further technical effect which goes beyond the 'normal' physical interactions between program (software) and computer (handware), it's not excluded from patentability. See Paterson, G. (2001). *The European patent system: The law and practice of the European Patent Convention*. London: Sweet & Maxwell, at 418-419.
[6] See Arezzo, E., & Ghidini, G. (2011). *Biotechnology and software patent law: A comparative review of new developments*. Cheltenham: Edward Elgar, at 131.
[7] See Arezzo, E., & Ghidini, G., *supra note 6*, at 131.

you wish to protect from your competitor may differ is depending on how the software is used together with the hardware.[8]

Third, the Internet raises complex issues regarding the enforcement of patents. In our information age, the protection of data is tremendously important because data is rampantly collected via the internet and evaluated by companies for commercial purposes. Even the world's leading corporations are accused of breaching consumers' data privacy.[9] Thus, should we define the term "use" in privacy same as in patent infringement? In this article, I will introduce some decisions in American and Taiwanese courts about this.

THE IMPORTANCE OF PATENT AND PRIVACY PROTECTION IN TAIWAN CONSTITUTION

To promote industrial development, most countries make laws to grant patents for new inventions having industrial applicability or new models or improvements in the design, construction or fitting of an object having practicality so as to encourage inventiveness and creativity.[10]

The granting of patent rights concerns the interests of the applicant and interested parties. It also has a bearing on the interest of the public. To preserve human dignity and to respect free development of personality is the core value of the constitutional structure of free democracy, the right of privacy will also affect the interest of the public. This right is not among those rights specifically enumerated in the Taiwan Constitution (hereinafter "this Constitution"), [11] whereas it should nonetheless be considered as an indispensable fundamental right and thus protected under Article 22 of the Constitution for purposes of preserving human dignity, individuality and moral integrity, as well as preventing invasions of personal privacy and maintaining self-control of personal information.[12]

As far as the right of information privacy is concerned, which regards the self-control of personal information, it is intended to guarantee that the people have the right to decide whether or not to disclose their personal information, and, if so, to what extent, at what time, in what manner and to what people such information will be disclosed. It is also

[8] See http://www.wipo.int/sme/en/documents/software_patents_fulltext.html (accessed March 2015).
[9] See Jörg Binding (2012). Protecting the consumer. *China Law & Practice*, 25(10), 12.
[10] See J. Y. Interpretation No. 213.
[11] In US, strictly speaking, the word "privacy" doesn't also appear in the Declaration of Independence, U.S. Constitution, or the Bill of Rights, nor in any of the seventeen amendments added to U.S. Constitution since. See Lane, F. S., *supra note 1*, at 15.
[12] See J. Y. Interpretation No. 585.

designed to guarantee that the people have the right to know and control how their personal information will be used, as well as the right to correct any inaccurate entries contained in their information.

THE MEANING OF "USE" IN PATENT INFRINGEMENT

When we did our reports, we might search some statistics and copy the results. For example, to let the back-end system provide a result for download, we create a query to seek particular and specified information. If the search engine is similar to someone's patent, are we infringing it?

In the Centillion decision,[13] the patent at issue in Centillion disclosed a system for collecting, processing, and delivering information from a service provider, such as a telephone company, to a customer. The claim involved both a "back-end" system maintained by the service provider and a "front-end" system maintained by an end user, e.g., a customer. The most interesting part of this decision is whether customers had "used", so let's talk about it.

First, what is infringement of patent? According to 35 U.S.C. § 271 (a) (hereinafter "Section 271(a)"), except as otherwise provided in this title, whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent.

Then, we should realize the meaning of "use" a system. The Federal Circuit held that "to 'use' a system for purposes of infringement, a party must put the invention into service, i.e., control the system as a whole and obtain benefit from it."

Applying these principles, the Federal Circuit held that the customer "used" the system under Section 271(a). Specifically, the Federal Circuit found the user who initiated demand for the service caused the service provider's back-end system to generate the requisite reports as a result. The Federal Circuit explained that this was "use" because "but for the customer's actions, the entire system would never have been put into service."

Because the Federal Circuit noted that the customers "use" the system as a matter of law does not settle the issue

[13] See Centillion Data Systems, LLC v. Qwest Communications Intern., Inc., 631 F.3d 1279, 97 U.S.P.Q.2d 1697.

of infringement, they refused to decide whether the accused products satisfy the "as specified by the user" limitations for the first time on appeal.[14]

Though the Federal Circuit made no comment on whether Qwest may have induced infringement by a customer, we still pay attention to whether the system we are using infringes a patent.[15]

THE GUARDIAN OF PERSONAL INFORMATION IN TAIWAN

To protect bank customers' confidential information on their individual properties and to prevent banks from freely and unilaterally disclosing such information,[16] with a view to protect the people's right of privacy, should we adjust its meaning when we define the use of patent infringement and illegal using of personal information? Before we discuss about the meaning of use in privacy, we might realize what make it become so vital. Hence, let's talk about the guardian of personal information in Taiwan at first.

Nevertheless, Fingerprints are biological features of an individual's person and are characterized by personal uniqueness and lifetime unchangeability. If the State intends to engage in mass collection of the people's fingerprinting information,[17] such information collection should use less intrusive means substantially related to the achievement of a compelling public interest, which should also be clearly prescribed by law, so as to be consistent with the intent of Articles 22 and 23 of the Constitution. Furthermore, they will become a form of personal information that is highly capable of performing the function of identity verification once they are connected with one's identity.

---

[14] Practical considerations such as managing and paying for litigation with many defendants, bad publicity, and alienating potential customers, often override any benefits that might come from suing unlicensed users of a patented invention. If there are few users of a very specialized invention, however, then suing users may be a viable strategy. See Thiele, A. R., Blakeway, J. R., Hosch, C. M., & American Bar Association. (2010). *The patent infringement litigation handbook: Avoidance and management*. Chicago, Ill: American Bar Association, at 98.

[15] If this action involved large numbers of infringers who are similarly situated, it might become a class action.

[16] Thanks to the Internet, collecting and analyzing customer data is easier and more widespread than ever before. Though the practice of collecting data about consumers is decades old, the Internet and its ability to collect data so easily have spurred new protests from privacy groups. Consumer concerns are greater on-line because the collection is a little less obvious. See Marcella, A. J., & Stucki, C. (2003). *Privacy handbook: Guidelines, exposures, policy implementation, and international issues*. Hoboken, N.J: J. Wiley, at 206.

[17] In US, technology is available that would allow legal residents to carry a card containing a computer chip that could hold a considerable amount of personal information, such as fingerprint images. See Marcella, A. J., & Stucki, C., *supra note 16*, at 232.

In Fingerprints case,[18] the legislative goal of Article 8 of the Household Registration Act as promulgated and implemented in 1997 might be to establish fingerprinting data of all the people so as to "verify personal identity," "to identify stray people, roadside patients, feebleminded senior citizens and unidentified corpses," as well as to prevent false claim of another's identity card.

Because fingerprints possess such trait as leaving traces at touching an object, they will be in a key position to opening the complete file of a person by means of cross-checking the fingerprints stored in the database. As fingerprints are of the aforesaid characteristics, they may very well be used to monitor an individual's sensitive information if the State collects fingerprints and establishes databases by means of identity confirmation.[19]

Where it is necessary for the State to engage in mass collection and storage of the people's fingerprints and set up databases to keep same for the purposes of any particular major public interest, it shall not only prescribe by law the scope and means of such collection, which shall be necessary and relevant to the achievement of the purposes of such major public interest, but also prohibit by law any use other than the statutory purposes.[20]

However, the risk is that the information on the cards and vast storehouses of personalized data on each individual that the cards are linked to could be misused.[21] Even if the means is considered useful in achieving the aforesaid objectives in the future, Justices of the Constitutional Court, Judicial Yuan held that "still it fails to achieve balance of losses and gains and uses excessively unnecessary means, which is not in line with the principle of proportionality and thus infringes upon the people's right of information privacy as protected under Article 22 of the Constitution, when it compels all those above fourteen to be fingerprinted in advance and subjects them to those potential risks that may arise from unclear and indefinite delegation of power and unwarranted disclosure of fingerprinting information simply because of the needs to verify the identity of a roadside unconscious patient, stray imbecile or unidentified corpse."

Since article 8 of the Household Registration Act as promulgated and implemented in 1997 is in conflict with the

---

[18] See J. Y. Interpretation No. 603.

[19] Personal privacy is at risk not only when the government wants to do more for its citizens(such as provide Social Security benefits) but also when it allegedly wants to do less. See Lane, F. S. , *supra note 1*, at 214-215.

[20] The fundamental question, which too often goes unasked, is whether a particular agency is collecting the minimum amount of information necessary for its mission and no more. See *ibid*, at 260.

[21] See Marcella, A. J., & Stucki, C., *supra note 16*, at 233.

Constitution, according to Article 171 Paragraph 1 of the Constitution, it shall be null and void. Consequently, when the government agency doesn't use the personal information in accordance with the scope of its job functions provided by laws and regulations, and in compliance with the specific purpose of collection, it might breach people's privacy.[22]

THE MEANING OF "USE" IN PERSONAL INFORMATION PROTECTION ACT

For most business, good privacy practice doesn't mean never gathering information, using it, or sharing it.[23] As difficult as protecting medical privacy has proven to be, the issue of protecting consumers from marketers, information brokers, direct mailers, and the new generation of "cyberstallkers," is even more problematic.[24]

Take, as an example, the patent at issue in Centillion decision. It is a system for collecting, processing, and delivering billing data from a service provider to a customer. If their financial data[25] is manipulated or deleted by an intruder, it will lead to years of stress and headache, and perhaps even possible financial ruin.[26]

In order to prevent companies from selling or trading individuals' personal information without those individuals' knowledge or consent,[27] we should comprehend the meaning of use in Personal Information Protection Act in Taiwan (hereinafter "this Law").[28]

Compared to the meaning of use in the Centillion decision (See Exhibit 1), this Law defines use are all methods of

---

[22] In US, the potential for the abuse of centralized government databases has been controversial since at least the 1960s, when the Johnson administration proposed creating a National Data Center that would merge the data about individual American collected by twenty different federal agencies into a single computer database. See Sykes, C. J. (1999). *The end of privacy*. New York: St. Martin's Press, at 44.

[23] The companies that succeed will be those that figure out just how much privacy—and personalized attention—their customers really want. See Marcella, A. J., & Stucki, C., *supra note 15*, at 203; A Jupiter Media Metrix report released in August 2001, suggests companies can win the trust of Web users over time. The survey found more than 30% of long-time Web users trusted merchants and banks enough to give them personal information, while only 13% of people who've been online less than a year had that same level of trust. See http://www.informationweek.com/privacy-can-businesses-build-trust-and-exploit-opportunity/d/d-id/1011510? (accessed March 2015).

[24] See Sykes, C. J., *supra note 22*, at 247.

[25] Pursuant to Article 2 Subparagraph 1 of Personal Information Protection Act in Taiwan, the personal information includes the name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information which may be used to identify a natural person, both directly and indirectly.

[26] See Cronin, K. P., & Weikers, R. N. (2002). *Data security and privacy law: Combating cyberthreats*. St. Paul, Minn.: West., at 1-45.

[27] See Marcella, A. J., & Stucki, C., *supra note 16*, at 241.

[28] Compared to China, due to a lack of data protection regulation, the commercial misuse of data is common. See Jörg Binding, *supra note 9*, 12.

personal information use other than to record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit information for the purpose of establishing or using a personal information file.

Exhibit 1- Use in dictionary[29]

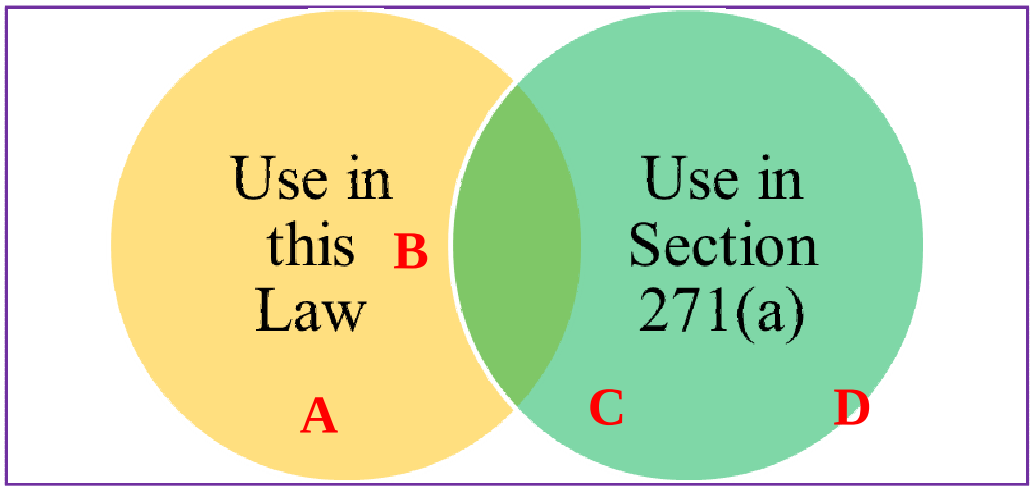

Exhibit 2- The different definition of use will affect the decision

Application	Use in this Law	Use in Section 271(a)	Decision
Case A	v	x	Only apply to this Law
Case B	v	v	Apply to both regulation
Case C	x	v	Only apply to Section 271(a)
Case D	x	x	Innocent

CONCLUSIONS

As Frederick S. Lane had said "If everyone throws a single soda can out of the car window, it does not take no long for a highway to look pretty hideous." We have been casually tossing bits of personal information out into the world for decades, while we should pay attention to not only patent but also privacy.

For instance, if a country provides limited protection of intellectual property rights, companies will encounter problems in enforcing their IP and have difficulty obtaining measures against increasingly sophisticated and organized counterfeiters.[30]

[29] See http://www.thefreedictionary.com/use (accessed March 2015).
[30] See Giovanni Guglielmetti, IP in China: Signs of improvement, available at http://www.worldipreview.com/article/ip-in-china-signs-of-improvement?utm_source=World+IP+Review&utm_campaign=81963a7234-WIPR_Digital_Newsletter_20_03_2015&utm_medium=email&utm_term=0_d76dcadc01-81963a7234-27407809(accessed March 2015)

Accordingly, due to the importance of self-control of personal information, when we define the meaning of use in patent infringement, which is relevant to personal information, we couldn't let someone unable to infringe the patent but capable of using personal information illegally (See Case A in Exhibit 2) .

To sum up, with market forces and regulation, we hope to make balance in defining the meaning of use in patent and privacy protection.

REFERENCES

1. Lane, F. S. (2009). *American privacy: The 400-year history of our most contested right*. Boston, Mass: Beacon Press.
2. Sean Sposito, Goodbye, billfold. Hello, smartphone, available http://www.ajc.com/news/business/personal-finance/goodbye-billfold-hello-smartphone/nfXNc/(accessed March 2015).
3. Paterson, G. (2001). *The European patent system: The law and practice of the European Patent Convention*. London: Sweet & Maxwell.
4. Arezzo, E., & Ghidini, G. (2011). *Biotechnology and software patent law: A comparative review of new developments*. Cheltenham: Edward Elgar.
5. http://www.wipo.int/sme/en/documents/software_patents_fulltext.html (accessed March 2015).
6. Jörg Binding (2012). Protecting the consumer. *China Law & Practice*, 25(10), 11-13.
7. Thiele, A. R., Blakeway, J. R., Hosch, C. M., & American Bar Association. (2010). *The patent infringement litigation handbook: Avoidance and management*. Chicago, Ill: American Bar Association.
8. Marcella, A. J., & Stucki, C. (2003). *Privacy handbook: Guidelines, exposures, policy implementation, and international issues*. Hoboken, N.J: J. Wiley.
9. http://www.informationweek.com/privacy-can-businesses-build-trust-and-exploit-opportunity/d/d-id/1011510?

(accessed March 2015).

10. Cronin, K. P., & Weikers, R. N. (2002). *Data security and privacy law: Combating cyberthreats*. St. Paul, Minn.: West.

11. http://www.thefreedictionary.com/use (accessed March 2015).

12. Giovanni Guglielmetti, IP in China: Signs of improvement, available at http://www.worldipreview.com/article/ip-in-china-signs-of-improvement?utm_source=World+IP+Review&utm_campaign=81963a7234-WIPR_Digital_Newsletter_20_03_2015&utm_medium=email&utm_term=0_d76dcadc01-81963a7234-27407809(accessed March 2015)